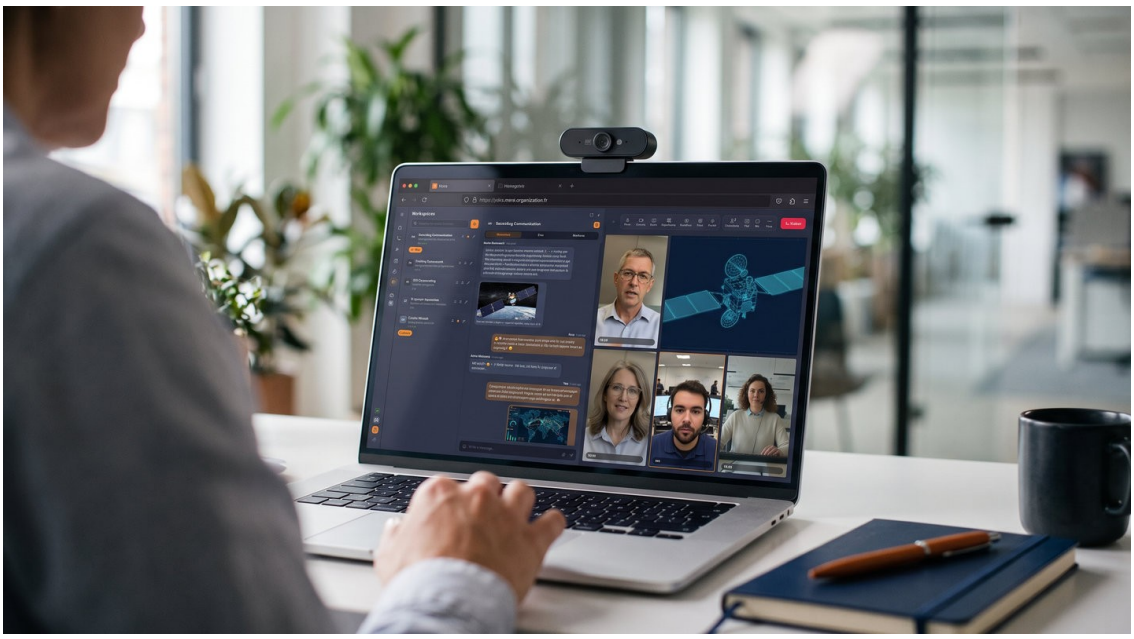
Press release
Montpellier, 12 October 2026

Tixeo launches version 18.2 of its collaboration platform: post-quantum protection comes to the browser

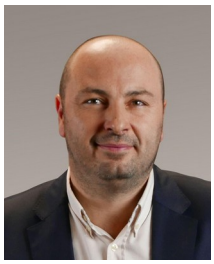
The platform's most open access point becomes its most protected.



(Above: an illustration of Tixeo V18.2; photo credit @Tixeo.)

Tixeo, the European provider of secure collaborative videoconferencing solutions whose technology has been awarded the First Level Security Certification (CSPN) four times by ANSSI, France's Cybersecurity Agency, today unveils version 18.2, combining a high level of security with seamless access. Accessible in a single click from the browser, the platform now adds post-quantum protection to its end-to-end encryption. European and sovereign, it is designed especially for critical and sensitive sectors (defence, industry, energy, public administration, healthcare, finance, etc.).

Version 18.2 requires no new installation, for employees and external participants alike. A simple link is all it takes to join a meeting and access the platform's collaboration features (real-time transcription and translation, file sharing, chat, Workspaces, etc.).



"ANSSI plans to make the integration of post-quantum mechanisms a condition of its certifications from 2027. Tixeo has chosen to get ahead of that deadline," says **Renaud Ghia, CEO of Tixeo**.

“In most videoconferencing solutions, the browser is where end-to-end encryption fades away. At Tixeo, it is where it goes furthest,” he continues.

End-to-end encryption strengthened with post-quantum protection

Tixeo is strengthening the end-to-end encryption of its platform with post-quantum protection in the browser. The exchange that establishes each meeting’s key combines the established X25519 mechanism with the post-quantum ML-KEM-768 mechanism, designed to withstand the quantum computers of tomorrow.

This hybrid exchange protects every stream in the meeting (audio, video, screen sharing, chat, file transfer) as well as Workspaces (virtual open-plan office, messaging, file storage and sharing, during and outside meetings). It runs on Tixeo’s own encryption engine, without relying on any primitive provided by the browser or the operating system.

Post-quantum protection applies whenever all participants, whether in a meeting or in a Workspace, are connected from a browser running V18.2. If any of them uses the application or an earlier version, the exchange relies on the standard end-to-end encryption mechanism.

“*In the enterprise videoconferencing market, the few post-quantum protections available today come from US providers. Yet they remain subject to the CLOUD Act, which can compel them to comply with access requests from US authorities. With V18.2, Tixeo brings this post-quantum protection to a European, sovereign platform, with no exposure to extraterritorial legislation,*” notes **Renaud Ghia**.

A smooth, intuitive experience, straight from the browser

“Sensitive organisations want collaboration tools that are as easy to use as the ones they are used to, without compromising the security of their communications. That twofold requirement guided the development of our V18.2: a familiar interface that users can pick up immediately, while maintaining the level of protection their activities demand,” adds **Renaud Ghia**.

During a call, Picture-in-Picture mode displays participants in a floating window as soon as the user switches to another tab. Messaging can be expanded to fill all or part of the screen, becoming a fully fledged space for exchange in its own right. Fusion mode and Workspaces become even smoother, just like a real open-plan office. Files and history remain at hand: meeting, workspace and documents all fit in a single tab.

Tixeo enriches this experience with real-time transcription and translation of conversations, displayed as subtitles and powered by sovereign AI. In an international meeting, every participant can follow the discussion live in their own language.

“With V18.2, we are applying a principle that has guided our R&D for more than twenty years: treating tomorrow’s security requirements as today’s constraints, without making things harder for users. As ANSSI’s doctrine takes shape between now and 2027, Tixeo will continue to extend its post-quantum scope,” says **Renaud Ghia**.

Available from the browser, post-quantum protection will be extended across the entire Tixeo ecosystem over the coming months, starting with the mobile app and then the native client,

with the same commitment to simple access and ease of use. Roll-out of version 18.2 will begin in the coming days.

Going further…

The fundamentals of Tixeo encryption

- **Keys are generated and stored on participants' devices**. The server never holds them.
- **Streams are encrypted on the sender's device and decrypted only on the recipients' devices.** The server routes sealed data that it cannot read.
- **Proprietary encryption developed by Tixeo**, a European vendor: no third-party dependency, no backdoor, no exposure to extraterritorial legislation.
- **Enabled by default across all exchanges** (audio, video, screen sharing, messaging, files, Workspaces), whatever the number of participants, with no security settings to configure.
- **The same technology runs in the browser with V18.2**: encryption is performed client-side, within Tixeo's own engine.
- **External participants, with no account or installation, benefit from the same protection.**
- **The organisation stays in control**: browser access is enabled server-side and authorised by security profile.

Tixeo post-quantum protection: the mechanism at a glance

- **Each meeting's key establishment becomes hybrid: X25519** (elliptic curves) + **ML-KEM-768** (FIPS 203 standard). Nothing is replaced: the classical mechanism remains in place and the post-quantum mechanism is added to it.
- **Aligned with ANSSI doctrine**: ANSSI's ANSSI-PG-083 guide requires hybridisation for any product aiming for post-quantum security. Tixeo's construction corresponds to the mode this guide considers the most desirable. Tixeo can therefore rely on the guide itself.
- **Scope**: browser only at this stage, in meetings (audio, video, screen sharing, chat, instant file transfer) and in Workspaces (virtual open-plan office, messaging, file storage and sharing, during and outside meetings), provided that all participants are connected from a browser.
- **Enabled by default, with no degraded mode**. Nothing to activate, no configuration prerequisites. Protection applies between two 18.2 web clients; when a participant connects from the application or uses an earlier version, the exchange falls back to the classical mechanism.

For more details on how post-quantum protection works and on the browser access architecture, a technical appendix is available here.

PRESS CONTACTS | OXYGEN (French PR agency)
Eliot Granveau - eliot.g@oxygen-rp.com - +33 6 26 36 41 17
Caroline Hoffmann - caroline.h@oxygen-rp.com

About Tixeo

For more than 20 years, Tixeo, a European provider of secure collaborative videoconferencing solutions, has supported strategic organisations (defence, industry, energy, etc.) in ensuring the efficiency and security of their online exchanges as part of their critical activities.

Available in the cloud or on-premise, Tixeo offers its own videoconferencing technology, awarded the CSPN certification four times by ANSSI, which complements standard collaboration tools for even greater confidentiality. Built on a Secure by Design approach, its technology features genuine end-to-end encryption of all streams (video, audio, data), whatever the number of participants.

With an unprecedented level of security, Tixeo helps organisations reduce cyber risk, strengthen cyber resilience and meet regulatory requirements. Many European organisations place their trust in Tixeo, including Naval Group, Dassault Aviation, Orange, Orano and Bordeaux Airport.

Tixeo holds the ‘Cybersecurity Made in Europe’ label.

Find out more: www.tixeo.com